

SEALED

UNITED STATES DISTRICT COURT

for the
Western District of Virginia

JUN 24 2016

JULIA C. DUDLEY, CLERK
BY: *K. Eaton*
DEPUTY CLERK

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)EMAIL ACCOUNTS TPETER424@GOOGLEMAIL.COM, NOVDEC21@GMAIL.COM,
VEGAX2017@GMAIL.COM, TIM.VEGAX@GMAIL.COM AND
DRPAULM7@GMAIL.COM
THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE

Case No. 5:16mj00023

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the WESTERN District of VIRGINIA, there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 USC 331(a)	introduction of misbranded drugs or devices into interstate commerce;
18 USC 1341	wire fraud; and
18 USC 1028	aggravated identity theft.

The application is based on these facts:
SEE AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT, INCLUDED BY REFERENCE
HEREIN

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 120 days (give exact ending date if more than 30 days: 10/21/16) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Received by reliable electronic
means and sworn and attested to
by telephone.*Michael Kursky*

Applicant's signature

Michael Kursky, Special Agent, FDA-OCI

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/24/16

Charlottesville, VA

City and state: Harrisonburg, VA*Joel C. Hoppe*

Judge's signature

HONORABLE JOEL C. HOPPE, MAGISTRATE JUDGE

Printed name and title

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH THE EMAIL ACCOUNTS
TPETER424@GOOGLEMAIL.COM,
NOVDEC21@GMAIL.COM,
VEGAX2017@GMAIL.COM,
TIM.VEGAX@GMAIL.COM AND
DRPAULM7@GMAIL.COM THAT ARE STORED AT
PREMISES CONTROLLED BY GOOGLE

Case No. **5:16mj00023**

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Michael Kurisky, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an Application for a Search Warrant for information associated with the email accounts **tpeter424@googlemail.com,** **novdec21@gmail.com,** **vegax2017@gmail.com,** **tim.vegax@gmail.com** and **drpaulm7@gmail.com** that are stored at premises controlled by Google, an Internet service provider headquartered at 1600 Amphitheatre Way, Mountain View, CA. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been a Special Agent with the Food and Drug Administration's Office of Criminal Investigations ("FDA-OCI") since November 2002 and am currently assigned to the Metro Washington Field Office. Between September 2010 and November 2012, I worked as a

Special Agent with the Department of Veterans Affairs Office of Inspector General. Before working at FDA-OCI, I served as a Special Agent with the United States Secret Service. In my law enforcement career, I have continually trained on criminal investigative techniques, and have completed courses including the Special Agent Training Program at the Federal Law Enforcement Training Center, the United States Secret Service Special Agent Training Course, and the FDA-OCI Special Agent Training Course. I also graduated from the Virginia Commonwealth University in Richmond, Virginia, with a degree in criminal justice. At FDA-OCI, I conduct criminal investigations, make arrests, and execute search and seizure warrants for Title 18 offenses as well as crimes involving violations of the Federal Food, Drug, and Cosmetic Act (the "FDCA"), codified at 21 U.S.C. §§ 301-395.

3. This Affidavit is merely intended to show that there is sufficient probable cause for the requested warrant; it does not set forth all of my knowledge about this matter.

4. Based on my training and experience in conjunction with the facts in this Affidavit, I submit that there is probable cause to believe that crimes including violations of 21 U.S.C § 331(a) (introduction of misbranded drugs or devices into interstate commerce), 18 U.S.C. § 1341(wire fraud), and 18 U.S.C. §670 (theft of medical products) and 18 U.S.C. § 1028A (aggravated identity theft), have been committed by the individuals associated with the email accounts **tpeter424@googlemail.com**, **novdec21@gmail.com**, **vegax2017@gmail.com**, **tim.vegax@gmail.com**, and **drpaulm7@gmail.com**. I submit that there is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTES AND DEFINITIONS

6. The FDA is the federal agency charged with protecting health and safety by enforcing the FDCA, which is a law ensuring that drugs sold for human use are safe and effective. The FDA regulates drug manufacturing, distribution, packaging, and labeling.

7. Under the FDCA, a “device” is an article intended for use in diagnosing diseases or other conditions, or in curing, mitigating, treating, or preventing disease in human beings, or is intended to affect the structure or any function of the body but which does not achieve its primary purposes through chemical action within or on the body of human beings and which is not dependent on being metabolized for the achievement of its primary intended purposes. 21 U.S.C. §§ 321(h)(2), (3).

8. Devices fall into one of three classes, with Class I requiring the least amount of controls and Class III requiring the greatest amount of controls. Class III devices require that the FDA approve a premarket application before being distributed in interstate commerce. A Class III device that is distributed in interstate commerce without an approved premarket application is “adulterated” under the FDCA.

9. *Introduction of misbranded drugs or devices into interstate commerce.*
Introducing misbranded drugs or devices into interstate commerce is a crime punishable by

imprisonment for not more than one year. Doing so with intent to defraud or mislead is a federal felony. *See* 21 U.S.C. §331(a).

10. *Wire Fraud.* Under 18 U.S.C. § 1343, whoever, having devised any scheme for obtaining money or property by means of false or fraudulent pretenses, transmits, or causes to be transmitted by means of wire, any writings, for the purpose of executing such scheme shall be fined or imprisoned not more than 30 years or both.

11. *Theft of Medical Products.* Under 18 U.S.C. § 670, whoever, embezzles, steals, or by fraud or deception obtains...a pre-retail medical product...if the value of the medical products involved in the offense is \$5,000 or greater, shall be fined under this title, imprisoned for not more than 15 years.

12. *Aggravated Identity Theft.* Under 18 U.S.C. § 1028A, whoever, knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

SUMMARY OF PROBABLE CAUSE

13. My preliminary investigation has turned up evidence that unknown suspects have orchestrated a fraud scheme using the identifiers of individuals employed by Valley Health D/B/A the Winchester Medical Center, which is an actual hospital located at 1840 Amherst Street, Winchester, VA. These individuals have created bogus internet domain names that give the impression they are affiliated with the Winchester Medical Center, and then reach out to various medical supply distributors across the United States and attempt to open lines of credit in the hospital's name. Account and credit applications completed by the suspects contain the names of both current and former Winchester Medical Center employees. Legitimate financial

disclosure forms associated with the hospital have also been submitted by the suspects, although it is unknown how or where they were obtained. Once these lines of credit are established, orders are placed for diabetic testing strips and other medical supplies. These orders are then shipped to locations across the Commonwealth of Virginia. The account applications contain email addresses created by the suspects that mimic the legitimate employees, but they come back to accounts created and controlled by the suspects. To date, orders were placed using the email addresses mark.baker@winchestermedicalcenter.org and todd.way@winchestermedicalcenter.org which resulted in fraudulently obtained medical devices being shipped. Mark Baker is the name of an actual employee at the Winchester Medical Center and Todd Way is a former employee at the Winchester Medical Center.

14. In May 2015, an individual identifying himself as Mark Baker, using the email address accounts@valleyhealthlink.org, contacted Seneca Medical located at 85 Shaffer Park Drive, Tiffin, Ohio and attempted to open an account in the name of Valley Health System D/B/A Winchester Medical Center. The subject listed a contact number of 540-252-3162. Along with the application was a copy of a pharmacy permit issued by the Virginia Department of Health Professions (VA-DHP). The subject indicated that he wished to purchase 1100 boxes of diabetic test strips and have them shipped to a warehouse located in Reston, VA. This shipment was flagged as fraudulent and was never sent. VA-DHP has confirmed that the pharmacy permit was not legitimate. At the time this attempt took place, there was a Mark Baker employed by Valley Health with the legitimate email address of mark.baker@valleyhealthlink.com. Public records show the registrant for the domain name valleyhealthlink.org is a company called Vista Print Technologies located in Bermuda.

Legitimate representatives of Valley Health confirmed that this was not a domain name associated with their business and that this application was not submitted by its employees.

15. In February 2016, a complaint was received by VA-DHP that a false pharmacy permit had been submitted to Matrix Distributors, located in East Brunswick, NJ. Subsequent investigation determined that someone attempted to open an account in the name of Winchester Medical Pharmacy. An email contact was provided for mark.baker@valleyhealthlink.net, and listed the contact number as 540-705-0770. VA-DHP confirmed that the pharmacy permit was not legitimate. Public records show the registrant for the domain name valleyhealthlink.net is Whois Privacy Protection Service located in Kirkland, Washington. Legitimate representatives of Valley Health confirmed that this was not a domain name associated with their business and that this application was not submitted by its employees.

16. In February 2016, an individual identifying himself as Mark Baker, using the email address mark.baker@winchestermedicalcenter.org and mark.baker@valleyhealthlinks.com, contacted Westminster Pharmaceuticals located in Olive Branch, MS, and submitted an application in the name of Valley Health System D/B/A Winchester Medical Center. Mark Baker provided a contact number of 540-705-0770. Also submitted with the application was a VA-DHP Pharmacy Permit in the name of Valley Pharmacy and Winchester Medical Pharmacy Center, both of which were confirmed as fraudulent by VA-DHP. Legitimate representatives of Valley Health confirmed that these were not domain names associated with their business and that this application was not submitted by its employees.

17. According to public records the registrant for the domain name valleyhealthlinks.com is listed as Mark Baker, 1840 Amherst Street, Winchester, VA, contact

number 540-705-0770. The registrant email address was listed as vegax2017@yahoo.com. The domain was created on 02/12/2016. Public records also show the registrant for the domain name winchestermedicalcenter.org as Mark Baker, 1108 Amherst Street, Winchester, VA, contact number 540-705-0770. The registrant email address was listed as vegax2017@yahoo.com. The domain name was created on 03/03/2016. Legitimate employees of Valley Health confirmed that neither domain name is associated with Valley Health or the Winchester Medical Center.

18. In March 2016, an individual identifying himself as Mark Baker, using the email address mark.baker@winchestermedicalcenter.org contacted NuCare Pharmaceuticals located in Orange, CA and created an account in the name of Winchester Medical Center, 1840 Amherst Street, Winchester, VA, contact number 540-705-0770. Along with the application was a Pharmacy Permit in the name of Winchester Medical Pharmacy Center, which has been confirmed as fraudulent by VA-DHP. The application was approved and a credit line was established. Mark Baker placed an order for various diabetic test strips in the amount of \$4350.20. These items were shipped on 03/14/2016 via FedEx Second day, tracking number 00639229197007 to 11815 Fountain Way, Suite 300, Newport News, VA. Legitimate employees of Valley Health confirmed that this was not an email, phone number, order or address associated with Valley Health, or the Winchester Medical Center.

19. In March 2016, information was received that a person identifying themselves as Todd Way, using the email address todd.way@winchestermedicalcenter.org, phone number 540-705-0770, contacted Henry Schein, a medical distributor, located in Melville, NY and opened an account in the name of Winchester Medical Center, 1840 Amherst Street, Winchester, VA. The account was approved and Todd Way placed two separate orders. On 03/15/2016 an order was placed for \$2967.19 worth of diabetic test strips and on 03/18/2016 a second order was placed

for \$3949.26 worth of diabetic test strips. Both shipments were sent to 4860 Cox Road, Glen Allen, VA. Legitimate employees of Valley Health confirmed that this was not an email, phone number, order or address associated with Valley Health, or the Winchester Medical Center.

20. On March 28, a preservation request was sent to Yahoo! via the email address lawenforcement-request-delivery@yahoo-inc.com for the email account vegax2017@yahoo.com.

21. On March 30, 2016, SA Kurisky met with the property manager of Business Center International (“BCI”), located at 4860 Cox Road, Suite 200, Glen Allen, VA, 23060, which was the shipping address for the fraudulent purchase from Henry Schein. BCI is a virtual office in which customers can open an account and receive a variety of services to include mail delivery and mail forwarding services. A review of the application submitted by Mark Baker shows this account was created on February 18, 2016, and he listed the following: phone number – 540-705-0770, address – 1840 Amherst Street, Winchester, VA 22601. The subject also submitted an insurance form from Hudson Insurance, and a Maryland driver’s license in the name of Mark Baker. Among the documents provided was an email dated February 17, 2016 sent from mark.baker@valleyhealthlinks.com with the subject line “New Account”, and two faxes sent from 540-750-4073.

22. Additionally, one of the documents provided from BCI was an email dated March 21, 2016, sent from vegax2017@yahoo.com to the BCI manager stating “Good morning peggy we have a package that is meant to be deliver this morning once you have them can you add the two together and place this label on it for shipment i have already scheduled a pickup..” The manager advised that the packages in question were the items received from Henry Schein. Attached to the email was a FedEx shipping label sending the package to Greenville, SC.

23. Based upon the above probable cause, a search warrant was issued for the email account vegax2017@yahoo.com. An analysis of that email account revealed that it was in communication with **tpeter424@googlemail.com**, **novdec21@gmail.com**, **vegax2017@gmail.com**, **tim.vegax@gmail.com** and **drpaulm7@gmail.com**. Furthermore, all communications between these accounts dealt strictly with the fraud scheme outlined above. There were no emails that would be characterized as “personal” in nature. Based on the preliminary analysis of the emails, I believe that there is probable cause to believe that each of these email accounts are involved in the scheme to assume the identities of various hospitals and its employees, produce fictitious documentation to include state pharmacy licenses, US State Department passports, Drug Enforcement Administration licenses in order to open lines of credit at medical distributors across the country, and pay for the costs associated with the scheme using stolen credit card numbers, and fraudulently obtain diabetic test strips and other medical products. For example:

TPETER424@GOOGLEMAIL.COM

24. The following emails were found in connection with the **tpeter424@googlemail.com** account:

- a. On February 11, 2016, **tpeter424@googlemail.com** sent an email to vegax2017@yahoo.com with the subject line “see”. The email contained a link to download Yahoo messenger as well as two American Express Credit Card numbers, the dates of expiration, the card verification value (CVV), the name of who it was issued, the address of the individual and a phone number for at least one of the individuals. Both numbers were forwarded to American Express

Global Security who advised that one of the numbers had not been reported lost / stolen, but that the second number had been reported as compromised.

- b. On March 5, 2016, vegax2017@yahoo.com sent an email to **tpeter424@gmail.com** with the subject line “v”. The email contained an attachment with the file name “CREDIT APPLICATION – Winchester Medical Center 1.pdf”. The attachment was a credit application with a company called Health Coalition located in Florida. The application had been filled out in the name of the Winchester Medical Center and listed the address of its distribution center as 900 Commonwealth Place, #200-349, Virginia Beach, VA, which is the location of a virtual office. The application listed the email address todd.way@winchestermedicalcenter.org and a contact number of 540-705-0770, both of which are known to be used by the suspects in this scheme and not associated with the legitimate Winchester Medical Center.
- c. On March 5, 2016, **tpeter424@gmail.com** sent an email to vegax2017@yahoo.com that contained five individual .jpgs of the Health Coalition application that contained the fictitious information. The only noticeable difference between the two files was that this one contained the alleged signatures of “Robert M Amos” who was listed as the CFO and “Michael Halseth” who was listed as the COO.

NOVDEC21@GMAIL.COM

25. The following emails were found in connection with the **novdec21@gmail.com** account:

- a. On February 14, 2016, an email was sent from mark.baker@valleyhealthlinks.com to vegax2017@yahoo.com and **novdec21@gmail.com** with the subject line "File Winchester" that contained three attachments. One of the attachments was an image of a Pharmacy Permit from the Virginia Department of Health Professions in the name of the Winchester Medical Pharmacy Center with license number 0201002043. A query of the Department of Health Professions website shows that license number as being assigned to the Manassas Pharmacy in Manassas, VA.
- b. On February 18, 2016, an email was sent from vegax2017@yahoo.com to **novdec21@gmail.com**. The email contained a .pdf that contained an application to open a mail box at Alliance Virtual Office, 900 Commonwealth Place, Suite 200, Virginia Beach, VA. The application was in the name of Mark Baker and listed a contact number of 540-705-0770. Also in the document was a copy of a Maryland Driver's license in the name of Mark Baker, containing license number R-560-275-866-969. A query with the State of Maryland shows this license number is issued to someone other than Mark Baker. Lastly, there was a document allegedly from Hudson Insurance Company showing a Mark Baker as having auto insurance coverage for two vehicles. Representatives from Hudson Insurance confirmed that this document is not authentic.
- c. On February 28, 2016, an email was sent from vegax2017@yahoo.com to **novdec21@gmail.com** and sharplink50@yahoo.com that contained a total of eight pharmacy licenses issued by the Virginia Department of Health Professions.

All eight were checked by the license number on the Department of Health Professions website and all eight were confirmed as fraudulent.

- d. On March 22, 2016, vegax2017@yahoo.com sent an email to sharplink50@yahoo.com and **novdec21@gmail.com** with the subject line "Label". The email contained twelve attachments; the majority of which were images of Fed-Ex Priority Overnight shipping labels listing the sender as Terri Calderon, 40th S. 7th Street, Suite 104, Minneapolis, MN, and the recipient as Ray White, 2345 East North Street, Suite 1108, Greenville, SC. One of the labels contained the Fed-Ex tracking number of 7758 1749 6080. This was the same label that was sent to the office manager of Business Center International in Glen Allen, VA, to be used to ship the diabetic test strips that were fraudulently obtained by the suspects from the Henry Schein medical distributor. The name Terri Calderon was also one of the names associated with an American Express credit card that was sent by aprilten21@yahoo.com to vegax2017@yahoo.com on April 6, 2016.

VEGAX2017@GMAIL.COM

26. The following emails were found in connection with the **vegax2017@gmail.com** email account:

- a. On February 12, 2016, vegax2017@yahoo.com received an email from Google's Gmail Team, indicating that the email address **vegax2017@gmail.com** had been created and was ready to use.
- b. On February 12, 2016, vegax2017@yahoo.com sent an email to **vegax2017@gmail.com** with the subject line "PROFILE". The email contained,

among other things, the contact number being used by the suspects - 540-705-0770 and the domain address www.valleyhealthlinks.com.

- c. On February 12, 2016, an email was sent to vegax2017@yahoo.com with a CC to **vegax2017@gmail.com** containing an invoice from a company called “webnames.ca” confirming the creation of the domain name www.valleyhealthlinks.com. Webnames.ca is a domain name registrar located in Canada.
- d. On February 14, 2016, vegax2017@yahoo.com sent an email to **vegax2017@gmail.com** with the subject line “WMC PROFILE”. The email listed information about the Winchester Medical Center, but included the contact number controlled by the suspects (540-705-0770) and email addresses controlled by the suspects to include mark.baker@valleyhealthlinks.com and todd.way@valleyhealthlinks.com. The contact email address for the company vice president and CFO – Robert Amos, was listed as **vegax2017@gmail.com**.
- e. On February 29, 2016, vegax2017@yahoo.com sent an email to **vegax2017@gmail.com** and sharplink50@yahoo.com with the subject line “SUNDAY” that contained the wording for various “go-byes” that was requesting the pricing for various diabetic test strips from “Mark Baker” at Winchester Medical Center. The email listed several of the virtual office addresses being used by the suspects and listed seven American Express credit card numbers along with the expiration date, CVV, cardholder’s name and address.

TIM.VEGAX@GMAIL.COM

27. The following emails were found in connection with the **tim.vegax@gmail.com** email account:

- a. On March 08, 2016, an email was sent to vegax2017@yahoo.com from the Google Gmail Team advising that the Gmail address **tim.vegax@gmail.com** had been created.
- b. Continuing on the same day, an email was sent from vegax2017@yahoo.com to vegax2017@yahoo.com (the same email address) with the subject line "Job offer". The message contained the email address **tim.vegax@gmail.com**, along with the following message:

"Hi hope your day is going on fine i have been waiting for your email forever but I guess u had wrong email...Anyway just a couple of things i needed to know before we get started..1.I need the full name and address with your regular cell phone preferred smart phone if not we might wanna get one later on..2. Do you have a whole day to yourself or you work part time? 3. Do you have a computer??? Cos we are going t be communicate more by email or instant messenger....If all this is fine we are good to go tell me what you need i will look into that anything at all....Thank you...." Based on a review of the emails in this case and knowledge of the nature of this and other similar fraud schemes, your affiant believes the suspects involved in this case have created this email account to attract "work from home" individuals who are used to receive and or collect the fraudulently obtained diabetic test strips and then re-ship those items to other addresses controlled by the suspects.

DRPAULM7@GMAIL.COM

28. The following emails were found in connection with the **drpaulm7@gmail.com** email account:

- a. On April 23, 2016, **drpaulm7@gmail.com** forwarded to vegax2017@yahoo.com a series of email conversations that occurred between **drpaulm7@gmail.com** and multisourcenational@gmail.com that took place between October 19, 2015 and November 15, 2015. (It should be noted that open source searches associate the email address multisourcenational@gmail.com with a company in Connecticut that purchases diabetic test strips.) The conversations discuss the selling of diabetic test strips to multisourcenational@gmail.com and payment methods. In one exchange from November 6, 2015, multisourcenational@gmail.com states "Sorry bud it seems you are either new to dts [Diabetic Test Strips] investing or you don't actually have the products. Everyone needs dates [expiration dates] before they buy. We can't purchase such large amounts outside(sic) if paypal if we can't confirm what you have exactly." In email exchanges on November 10, 2015, multisourcenational@gmail.com advises that he does wire transfers to Nigeria and to have the product mailed to an address in Springfield, Mass. **Drpaulm7@gmail.com** later provided information asking for payment be made to bank account in Nigeria via wire transfer to an account in the name of Dare Paul Alebiosu. The email forwarded to vegax2017@yahoo.com also contained three attachments which were images of Bank of America wire transfer authorization forms from the account of Multisource National Trading LLC to an account in Nigeria in the name of Dare Paul Alebiosu.

- b. On April 23, 2016, **drpaulm7@gmail.com** forwarded to vegax2017@yahoo.com and sharplink50@yahoo.com a series of email conversations that occurred between **drpaulm7@gmail.com** and multisourcenational@gmail.com that took place between December 31, 2015, 2015 and January 19, 2016. These conversations include **drpaulm7@gmail.com** stating the brand name and quantities of diabetic test strips that have been obtained and available for purchase and tracking numbers for shipments of diabetic test strips to Multi-Source National. During one email on January 4, 2016, **drpaulm7@gmail.com** states "giving you heads up i want 83k to go to the Nigeria account the rest will go to an American account i will provide to you if everything goes well...". On January 15, 2016, **drpaulm7@gmail.com** emailed "am giving you heads up for next Tuesday so you can be ready, so the cash won't be delayed i have 1200 One touch ultra 100 counts coming and 144 free style lite so be ready...". Attached to the email forwarded to vegax2017@yahoo.com and sharplink50@yahoo.com was an invoice for diabetic test strips in the amount of \$102,000 and three images of Bank of America wire transfer authorizations from Multi-Source National Trading to a company called Efusanya Services located in Rhode Island and to the account of Dare Paul Alebiosu in Nigeria.
- c. On April 23, 2016, **drpaulm7@gmail.com** forwarded to vegax2017@yahoo.com and aprilten21@yahoo.com a series of email conversations that occurred between **drpaulm7@gmail.com** and josh@multisourcenational.com between February 15, 2016 and March 23, 2016. In an email from March 7, 2016, **drpaulm7@gmail.com** states "I sent a package

by fedex 774975122295, its 25 Boxes of the one touch ultra 100 counts and 34 Boxes of the accu check 50 counts, Normally you know i do more than that...". On March 23, 2016, **drpaulm7@gmail.com** emailed josh@multisourcenational.com and stated "I have strips coming in today the total should be well over 8k but the rest will come in tomorrow the tracking for the tomorrow is 774975580299, so two packages are coming in today through fedex,so i want you to wire 8k,today,so we wont need to wire today and tomorrow...". [Agent note – Fed-Ex tracking number 774975580299 shows it originated in Greenville, SC on March 23, 2016. A fraudulent order for diabetic test strips from the Henry Schein medical distributor had been delivered to Greenville, SC on March 22, 2016.] Continuing on the same day, **drpaulm7@gmail.com** emailed josh@multisourcenational.com and stated "Yes see what you getting tomorrow...lolzz,,Below...30 Boxes of the One touch Ultra 100 counts, Free Style Lite 42 Boxes...". [Agent note – the fraudulently obtained shipment from Henry Schein contained a total of 42 Freestyle Lite diabetic strips.]

BACKGROUND CONCERNING E-MAIL AND DOMAINS

29. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google allows subscribers to obtain e-mail accounts at Google's registered domain name (Gmail), like the e-mail accounts listed in Attachment A. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as

account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. A Google subscriber can also store information files in addition to e-mails with the provider, such as: address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), Google Drive and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

31. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

32. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address

("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.


33. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

CONCLUSION

34. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Received by reliable electronic means and sworn and attested to by telephone on June 24, 2016.


Michael Kurisky
Special Agent, FDA-OCI

~~Subscribed and sworn to before me on June 24, 2016~~


JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH THE EMAIL ACCOUNTS
TPETER424@GOOGLEMAIL.COM,
NOVDEC21@GMAIL.COM,
VEGAX2017@GMAIL.COM,
TIM.VEGAX@GMAIL.COM AND
DRPAULM7@GMAIL.COM THAT ARE STORED AT
PREMISES CONTROLLED BY GOOGLE

Case No.

Filed Under Seal

Property to be Searched

This warrant applies to information associated with the email accounts

tpeter424@googlemail.com, novdec21@gmail.com, vegax2017@gmail.com,

tim.vegax@gmail.com and drpaulm7@gmail.com that are stored at premises controlled by

Google, a company that accepts service of legal process at 701 First Avenue, Sunnyvale, CA.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH THE EMAIL ACCOUNTS
TPETER424@GOOGLEMAIL.COM,
NOVDEC21@GMAIL.COM,
VEGAX2017@GMAIL.COM,
TIM.VEGAX@GMAIL.COM AND
DRPAULM7@GMAIL.COM THAT ARE STORED AT
PREMISES CONTROLLED BY GOOGLE

Case No.

Filed Under Seal

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the accounts, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 21 U.S.C § 331(a) (introduction of misbranded drugs or devices into interstate commerce), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 670 (theft of medical products) and 18 U.S.C. § 1028A (aggravated identity theft), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) All records related to the creation of false accounts to obtain misbranded medical devices.
- (b) The identity of the persons who created or used the user ID, including records that help reveal the whereabouts of such persons.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by **Google**, and my official title is _____. I am a custodian of records for **Google**. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of **Google**, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of **Google**; and
- c. such records were made by **Google** as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature